AMENDMENTS TO THE CLAIMS

1   1.   (CURRENTLY AMENDED) A computer-implemented method for executing an

2   untrusted program, comprising:

3   establishing a limited environment within a general environment, wherein said

4   limited environment comprises ~~at least~~ one or more mock resources ~~resource~~, wherein said

5   general environment comprises ~~at least~~ one or more real resources ~~resource, and~~ wherein

6   said limited environment and said general environment are both ~~implemented using~~

7   provided by the same ~~type of~~ operating system, and wherein programs executing within said

8   limited environment cannot access the one or more real resources in said general

9   environment;

10   executing at least a portion of an untrusted program within said limited environment;

11   and

12   examining said limited environment after execution of at least said portion of said

13   untrusted program to check for undesirable behavior exhibited by said untrusted program.

1   2.   (CANCELLED).

1   3.   (ORIGINAL) The method of claim 1, wherein said limited environment comprises a

2   shell in a UNIX operating system environment.

1   4.   (CURRENTLY AMENDED) The method of claim 1, wherein examining said

2   limited ~~mock~~ environment comprises:

3   determining whether ~~said~~ a particular mock resource of said one or more mock

4   resources has been deleted.

1   5.   (CURRENTLY AMENDED) The method of claim 1, wherein examining said

2   limited ~~mock~~ environment comprises:

3   determining whether ~~said~~ a particular mock resource of said one or more mock

4   resources has been renamed.

1   6.   (CURRENTLY AMENDED) The method of claim 1, wherein examining said

2   limited ~~mock~~ environment comprises:

3   determining whether ~~said~~ a particular mock resource of said one or more mock

4   resources has been moved.

1   7.   (CURRENTLY AMENDED) The method of claim 1, wherein examining said

2   limited ~~mock~~ environment comprises:

3   determining whether ~~said~~ a particular mock resource of said one or more mock

4   resources has been altered.

1   8.   (CURRENTLY AMENDED) The method of claim 7, wherein said particular mock

2   resource has a parameter associated therewith which changes when said particular mock

3   resource is altered, and wherein determining whether said particular mock resource has been

4   altered, comprises:

5   determining whether said parameter has changed.

1   9.   (CURRENTLY AMENDED) The method of claim 8, wherein said parameter is a

2   time value indicating when said particular mock resource was last updated.

1   10.   (CURRENTLY AMENDED) The method of claim 1, wherein examining said

2   limited mock environment comprises:

3   determining whether said particular mock resource has been accessed.

1   11.   (CURRENTLY AMENDED) The method of claim 10, wherein said particular mock

2   resource contains one or more sets of content, wherein said untrusted program executes in a

3   particular portion of memory, and wherein determining whether said particular mock

4   resource has been accessed comprises:

5   searching said particular portion of said memory for at least one of said one or more

6   sets of content.

1   12.   (ORIGINAL) The method of claim 1, further comprising:

2   providing information indicating behavior exhibited by said untrusted program.

1   13.   (ORIGINAL) The method of claim 12, wherein said information comprises

2   indications of undesirable behavior exhibited by said untrusted program.

1   14.   (ORIGINAL) The method of claim 1, further comprising:

2   determining whether said untrusted program has exhibited undesirable behavior; and

3   in response to a determination that said untrusted program has exhibited undesirable

4   behavior, taking corrective action.

1   15.   (ORIGINAL) The method of claim 14, wherein taking corrective action comprises:

2   deleting said untrusted program.

1   16.   (ORIGINAL) The method of claim 14, wherein taking corrective action comprises:

2   providing a warning to a user.

1   17.   (CURRENTLY AMENDED) A computer readable medium comprising instructions

2 which, when executed by one or more processors, cause the one or more processors to

3 execute an untrusted program, said computer readable medium comprising:

4   establishing a limited environment within a general environment, wherein said

5 limited environment comprises ~~at least~~ one or more mock resources ~~resource~~, wherein said

6 general environment comprises ~~at least~~ one or more real resources ~~resource, and~~ wherein

7 said limited environment and said general environment are both ~~implemented using~~

8 provided by the same ~~type of~~ operating system, and wherein programs executing within said

9 limited environment cannot access the one or more real resources in said general

10 environment;

11   executing at least a portion of an untrusted program within said limited environment;

12 and

13   examining said limited environment after execution of at least said portion of said

14 untrusted program to check for undesirable behavior exhibited by said untrusted program.

1   18.   (CANCELLED).

1   19.   (ORIGINAL) The computer readable medium of claim 17, wherein said limited

2 environment comprises a shell in a UNIX operating system environment.

1   20.   (CURRENTLY AMENDED) The computer readable medium of claim 17, wherein

2   said instructions for causing one or more processors to examine said limited ~~mock~~

3   environment comprises:

4   instructions for causing one or more processors to determine whether ~~said~~ a

5   particular mock resource of said one or more mock resources has been deleted.

1   21.   (CURRENTLY AMENDED) The computer readable medium of claim 17, wherein

2   said instructions for causing one or more processors to examine said limited ~~mock~~

3   environment comprises:

4   instructions for causing one or more processors to determine whether ~~said~~ a

5   particular mock resource of said one or more mock resources has been renamed.

1   22.   (CURRENTLY AMENDED) The computer readable medium of claim 17, wherein

2   said instructions for causing one or more processors to examine said limited ~~mock~~

3   environment comprises:

4   instructions for causing one or more processors to determine whether ~~said~~ a

5   particular mock resource of said one or more mock resources has been moved.

1   23.   (CURRENTLY AMENDED) The computer readable medium of claim 17, wherein

2   said instructions for causing one or more processors to examine said limited ~~mock~~

3   environment comprises:

4   instructions for causing one or more processors to determine whether ~~said~~ a

5   particular mock resource of said one or more mock resources has been altered.

1 24. (CURRENTLY AMENDED) The computer readable medium of claim 23, wherein

2 said particular mock resource has a parameter associated therewith which changes when

3 said particular mock resource is altered, and wherein said instructions for causing one or

4 more processors to determine whether said particular mock resource has been altered,

5 comprises:

6   instructions for causing one or more processors to determine whether said parameter

7 has changed.

1 25. (CURRENTLY AMENDED) The computer readable medium of claim 24, wherein

2 said parameter is a time value indicating when said particular mock resource was last

3 updated.

1 26. (CURRENTLY AMENDED) The computer readable medium of claim 17, wherein

2 said instructions for causing one or more processors to examine said limited mock

3 environment comprises:

4   instructions for causing one or more processors to determine whether said particular

5 mock resource has been accessed.

1 27. (CURRENTLY AMENDED) The computer readable medium of claim 26, wherein

2 said particular mock resource contains one or more sets of content, wherein said untrusted

3 program executes in a particular portion of memory, and wherein said instructions for

4 causing one or more processors to determine whether said particular mock resource has been

5 accessed comprises:

6   instructions for causing one or more processors to search said particular portion of

7 said memory for at least one of said one or more sets of content.

1 28. (ORIGINAL) The computer readable medium of claim 17, further comprising:

2   instructions for causing one or more processors to provide information indicating

3 behavior exhibited by said untrusted program.

1 29. (ORIGINAL) The computer readable medium of claim 28, wherein said information

2 comprises indications of undesirable behavior exhibited by said untrusted program.

1 30. (ORIGINAL) The computer readable medium of claim 17, further comprising:

2   instructions for causing one or more processors to determine whether said untrusted

3 program has exhibited undesirable behavior; and

4   instructions for causing one or more processors to, in response to a determination

5 that said untrusted program has exhibited undesirable behavior, take corrective action.

1 31. (ORIGINAL) The computer readable medium of claim 30, wherein said instructions

2 for causing one or more processors to take corrective action comprises:

3   instructions for causing one or more processors to delete said untrusted program.

1 32. (ORIGINAL) The computer readable medium of claim 30, wherein said instructions

2 for causing one or more processors to take corrective action comprises:

3 instructions for causing one or more processors to provide a warning to a user.

1 33. (CANCELLED).

1 34.   (CANCELLED).

1 35.   (CANCELLED).

1 36.   (CANCELLED).